North Country Hospital
Where caring runs deep.

189 Prouty Drive | Newport, VT 05855 | 802.334.7331

October 7, 2013

Dear :
We are sending you this letter to alert you to our discovery of a recent privacy breach that may involve your personal information. On September 18, 2013, we received notice that a former employee of the Hospital claims possession of a retired laptop that, unbeknownst to the Hospital, contains patient health information. The Hospital immediately demanded the return of the laptop, but the individual has failed and refused to return it.

Upon learning that this individual was in possession of the laptop with patient information and the individual's apparent refusal to return it, we immediately sought assistance from federal, state and local enforcement agencies to regain possession of the laptop to determine its contents – in particular what, if any, patient health information is stored on it. We contacted the Vermont Attorney General's Office on September 27, 2013 and the U.S. Attorney for the District of Vermont and the U.S. Department of Health and Human Services on September 27, 2013 and September 30, 2013 to report the situation. Simultaneously, we undertook efforts to identify what, if any, identifiable patient information was contained on the laptop. This effort is greatly complicated by the fact that the former employee has refused to provide us access to the laptop.

However, using other means, we have been able to identify the names of some individuals whose health information we believe is contained on the laptop, because it appears that it was unintentionally being stored in one particular employee's "My Documents" folder. This information, however, would only be accessible to an individual who had access to passwords used during the time period that the laptop was in service.

It is our belief that the former employee, by virtue of his previous position with the Hospital, has access to passwords necessary to view the information on the retired laptop. It is our belief that the patient health information on the laptop may include procedure summaries made between the dates of January 24, 2008 and July 3, 2012 by North Country OB/GYN services which may include information pertaining to you personally. Specifically, the information we believe that this former employee may have accessed includes name, procedure name, assisting surgeon, and start and end time for the procedure. We have not, however, received any indication that your personal information specifically has been used or disclosed by the former employee who has possession of the laptop or, as he has claimed, has placed it with his attorney to safeguard.

If you have questions or wish to learn additional information, please contact Andre Bissonnette, Compliance Officer, at 802-334-3253 or abissonnet@nchsi.org. We do not believe financial information was included on the laptop, but we have enclosed information with this letter on the steps you may take to protect yourself from financial harm. The hospital has taken steps to ensure that all patient health information is secure.

We are deeply disturbed by this situation, and we understand that this may be very unsettling for you. We sincerely apologize and regret that this situation has occurred. We will provide you with additional information should we learn more from the federal, state and local enforcement agencies. North Country Hospital is committed to providing quality care and to protecting your personal information. We want to assure you that we are taking every step to further improve policies and procedures to protect your privacy.

Sincerely,

André Bissonnette
VP of Finance / Compliance Officer

Steps to Consider for Financial Protection:

1. **Review your bank, credit card and debit card account statements** over the next twelve to twenty-four months and immediately report any suspicious activity to your bank or credit union.
2. **Monitor your credit reports** with the major credit reporting agencies.

Equifax	Experian	TransUnion
1-800-685-1111	1-888-397-3742	1-800-916-8800
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30374-0241	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

Under Vermont law, you are entitled to a free copy of your credit report from those agencies every twelve months. Call the credit reporting agency at the telephone number on the report if you find:

- Accounts you did not open.
- Inquiries from creditors that you did not initiate.
- Inaccurate personal information, such as home address and Social Security number.

3. If you do find suspicious activity on your credit reports or other account statements, call your local police or sheriff's office and file a report of identity theft.

4. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records, and also to access some services that are free to identity theft victims.

5. If you find suspicious activity on your credit reports or on your other account statements, consider placing a fraud alert on your credit files so creditors will contact you before opening new accounts. Call any one of the three credit reporting agencies at the numbers below to place fraud alerts with all of the agencies.

Equifax	Experian	TransUnion
888-766-0008	888-397-3742	800-680-7289

6. If you find suspicious activity on your credit reports **or on your other account statements, consider placing a security freeze on your credit report so that the credit reporting agencies will** not release information about your credit without your express authorization. A security freeze may cause delay should you wish to obtain credit and may cost some money to get or remove, but it does provide extra protection against an identity thief obtaining credit in your name without your knowledge. If you have Internet access and would like to learn more about how to place a security freeze on your credit report, please visit the Vermont Attorney General's website at:

http://www.atg.state.vt.us/issues/consumer-protection/identity-theft.php (or directly http://www.uvm.edu/consumer/?Page=idtheft.html).

You may also get information about security freezes by contacting the credit bureaus at the following addresses:

Equifax: https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

Experian: http://www.experian.com/consumer/security_freeze.html

TransUnion:

http://www.transunion.com/corporate/personal/fraudIdentityTheft/fraudPrevention/securityFreeze.page

7. If you do not have Internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

8. Even if you do not find suspicious activity on your credit report or your other account statements, it is important that you check your credit report for the next two years. Just call one of the numbers in paragraph 2 above to order your reports or to keep a fraud alert in place.

9. Helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report is available on the Vermont Attorney General's website at http://www.atg.state.vt.us. Another helpful source is the Federal Trade Commission website, http://www.ftc.gov/bcp/edu/microsites/idtheft/.